Cassandra Crossing/ Nuovi reati informatici

(29)— Italia verso l'adozione di reati come Detenzione abusiva di strumenti informatici o Uso illegale di dati criptati o steganografati…

Cassandra Crossing/ Nuovi reati informatici

Figure 1:

(29)— Italia verso l'adozione di reati come Detenzione abusiva di strumenti informatici o Uso illegale di dati criptati o steganografati. Saranno messi fuorilegge sistemi di brute force, Tor, Freenet e via dicendo?

31 marzo 2006—Alcune settimane fa si è svolto a Varenna un interessante convegno di giuristi, in cui tra le altre cose si è discusso della prossima riforma della parte del Codice Penale che si occupa di crimini informatici. Speravo che qualche addetto ai lavori commentasse alcuni aspetti preoccupanti di questo documento relativamente ai diritti civili in Rete ma, in sua assenza, tenterò di sostituirlo.

Il documento guida della discussione è stato il cosiddetto "Articolato Tanga", dal nome dell'autore principale. Riassume il lavoro della Commissione Nordio, che sta studiando il recepimento del trattato di Budapest ("Convenzione sulla cybercriminalità" del 23/11/2001) e della recente Direttiva Europea ("Decisione Quadro relativa agli attacchi contro i sistemi di informazione" del 19/4/2002) nella parte del codice penale italiano che attualmente tratta la cybercriminalità ed i reati informatici.

Si tratta di un documento interessante e ben scritto, che compie un evidente sforzo per comprendere e spiegare il mondo della Rete ad un uditorio che spesso lo conosce solo in maniera indiretta.

L'Articolato Tanga contiene, a parere di chi scrive, alcuni punti estremamente preoccupanti (per usare un eufemismo): due in particolare consistono nella definizione di nuove fattispecie di reato *"Detenzione abusiva di strumenti informatici"* e *"Uso illegale di dati criptati o steganografati"*.

Si tratta di due fattispecie di dubbia e comunque non dimostrabile efficacia nella repressione della criminalità, ma che possono certamente essere usate ed abusate anche per limitare e reprimere il diritto alla riservatezza ed alla libertà di espressione in Rete, e quindi come strumento di pressione psicologica nei confronti dei comportamenti di buona parte delle persone oneste che usano la rete come strumento di lavoro e di realizzazione personale.

Ma prima una parentesi doverosa per collocare quella che sarà una aspra critica all'Articolato Tanga. Proprio all'inizio, l'autore cita due brani della *"Dichiarazione di indipendenza del Cyberspazio"* di The Mentor (**John P. Barlow**). Questo documento, che è fondamentale per chiunque voglia capire la Rete, e la cui lettura è vivamente consigliata, ha una formulazione molto chiara e perentoria che, ad una lettura superficiale, può essere confusa con ingenuità o massimalismo.

Una maggiore attenzione, e magari una lettura comparata con la ben più famosa "Dichiarazione di Indipendenza" degli Stati Uniti permette invece di rivelare interessanti assonanze e punti di contatto in termini di libertà e diritti civili, chiare anche a "non informatici".

Il giudizio che l'autore dell'Articolato fornisce è chiaro e lapidario. Dopo aver citato la frase di The Mentor: "*Voi non conoscete la nostra cultura, la nostra etica, e nemmeno i codici non scritti che danno alla nostra società più ordine di quello che potrebbe essere ottenuto dalle vostre imposizioni*", l'autore commenta: "***Se tanta spocchia*** *induce al sorriso chi tratta quotidianamente con criminali efferati, nondimeno la questione è terribilmente seria".*

Considerare "spocchia" uno dei più famosi documenti della Rete a causa della sua forma, lascia pensare che il contenuto venga giudicato irrilevante o non sia stato nemmeno preso in considerazione. Questa sì è una questione seria e preoccupante.

Ebbene, vorrei commentare che il potere legislativo e quello giudiziario devono preoccuparsi prima di tutto degli onesti cittadini detentori dei diritti civili sanciti nella Costituzione della Repubblica Italiana, e pertanto indirizzare le loro attività istituzionali non solo contro il criminale ed in difesa della vittima del reato, ma anche tutelando tutti gli onesti ed innocenti. La formulazione delle due fattispecie di reato prima menzionate è invece quanto di più lontano possa immaginarsi da questo obbiettivo.

Cominciamo dalla **"Detenzione abusiva di strumenti informatici"**

La fattispecie di reato, definito di tipo anticipatorio, sancisce la illiceità del possesso di programmi destinati specificamente alla realizzazione di crimini informatici. Il testo stesso dell'articolato anticipa una critica elementare, facendo rilevare che la destinazione d'uso "tipica" di un programma per elaboratore può non essere questione facile da definire, essendo di tipo interpretativo.

Subito dopo però giustifica la cosa sostenendo che esistono programmi di funzionalità univoca (criminale), come i programmi di "Brute Force" destinati al crack delle password. Con ciò il giurista considera dimostrata la sua tesi, mentre per qualunque informatico è evidente che invece l'ha appena confutata.

I programmi di brute forcing, da "John the Ripper" in poi, fanno parte del set di strumenti indispensabili di qualunque esperto di sicurezza od amministratore di sistemi, che li usano per individuare gli utenti che hanno scelto password deboli. Da domani quindi, se il futuro della

legge italiana sul cybercrime sarà modellato con questi ragionamenti, sarà galera immediata per questi signori (io preferisco le arance, ricordatevelo se mi verrete a trovare).

Passiamo adesso all'altra fattispecie, **"Uso illegale di dati criptati o steganografati"**, definita così: "*Chiunque al fine di organizzare, o commettere o consentire che altri organizzino o commettano reati (…) trasmette, mediante un sistema di informazione, dati informatici criptati o steganografati".*

Mentre il testo sembra diretto a colpire le attività dei criminali e basta, in realtà colpisce anche i "fornitori" di servizi di comunicazione, cui viene sottratto il controllo sulle informazioni che trasmettono, in quanto crittografate. Poiché questi fornitori di servizi non sono più solo imprese, ma proprio nel caso di servizi volti alla tutela della privacy e dei diritti civili in rete sono singoli individui, spesso mossi da motivi idealistici ed altruistici, ciò equivale a vietare di fatto la realizzazione di server per la privacy, quali nodi Tor, Freenet o remailer anonimi.

E questo è il massimo effetto che il legislatore può ottenere, essendo nell'impossibilità di vietare "tout court" i sistemi crittografici visto che essi permeano ormai tutta l'informatica; pensiamo ad applicazioni quali la firma digitale o l'e-commerce.

Si potrebbe continuare, perché l'articolato contiene altre questioni di base, quali la parificazione tra immagini reali ed immagini virtuali al fine della commissione di reati legati alla pornografia minorile, in cui quindi il reato apparente e quello reale vengono kafkianamente equiparati, ma la trattazione si allungherebbe molto.

Sono sicuro che l'Articolato Tanga sia soprattutto il frutto di un lavoro onesto e professionale di chi ha per scopo principale quello consentire la repressione dei reati. Come in tutte le cose, la soluzione che verrà individuata dovrebbe essere frutto del bilanciamento tra questi e quei giuristi e legislatori che hanno il diritto, ed istituzionalmente anche il dovere, di difendere i diritti civili costituzionali dei cittadini. Si tratta pero' di una classe di persone che, particolarmente dopo l'11 settembre, pare andata in vacanza in tutto il mondo.

Chi può allora fare da forza equilibratrice?

Chi eviterà che vengano commessi errori grossolani con risultati liberticidi e di incertezza del diritto terrificanti?

Originally published at punto-informatico.it.

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica "Quattro chiacchiere con Cassandra"
Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero

By Marco A. L. Calamari on November 3, 2023.

Canonical link

Exported from Medium on August 27, 2025.